Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP05/001817

International filing date: 22 February 2005 (22.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: DE
Number: 10 2004 009 065.3
Filing date: 23 February 2004 (23.02.2004)

Date of receipt at the International Bureau: 27 April 2005 (27.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 10 2004 009 065.3

Anmeldetag: 23. Februar 2004

Anmelder/Inhaber: Stefan Kistner, 53840 Troisdorf/DE

Bezeichnung: Verfahren zur Verhinderung des Verlustes der Vertraulichkeit von Daten auf oder mit wechselbaren Speichermedien (Datenträgern)

IPC: G 06 F 12/16

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 12. April 2005
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Siedl

A 9161
03/00
EDV-L

Stefan Kistner
Kölner Straße 132
53840 Troisdorf

22.02.04

Titel

Verfahren zur Verhinderung des Verlustes der Vertraulichkeit von Daten auf oder mit wechselbaren Speichermedien (Datenträgern).

Anwendungsgebiet

Die Erfindung betrifft ein Verfahren zur Verhinderung des Verlustes der Vertraulichkeit von Daten

a.) durch nicht legitimierten Einsatz wechselbarer Speichermedien;

b.) bei Verlust wechselbarer Speichermedien.

Stand der Technik

[redacted]rbeitsplatzcomputer verfügen zunehmend über Schnittstellen, über die ein unkontrollierter [redacted]nd i.d.R. unerwünschter Datenaustausch mittels wechselbarer Speichermedien stattfinden kann. Die Abschaltung dieser Schnittstellen ist nicht praktikabel, da sie - wie z. B. die USB Schnittstelle - zum Anschluss von Peripheriegeräten erwünscht sind.

Der Transport und die Aufbewahrung wechselbarer Speichermedien erfordern besondere Sicherheitsmaßnahmen um ein unbefugtes Lesen (oder Kopieren), und damit den Verlust der Vertraulichkeit, zu verhindern. Als sinnvolle Maßnahme steht die kryptografische Verschlüsselung zur Verfügung.

Nachteile des Standes der Technik

Der Stand der Technik erlaubt es, ohne spezifische technische Kenntnisse, Speichermedien an Computer anzuschließen. Mit der quasi ubiquitären Verfügbarkeit nimmt die Gefahr des missbräuchlichen Einsatzes stetig zu. Dieser Gefahr stehen keine administrativen Kontrollmechanismen gegenüber.

Auf die insbesondere von der USB Schnittstelle ausgehenden Gefahren weist der Arbeitskreis [redacted]Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in seiner [redacted]chrift „Orientierungshilfe Datensicherheit bei USB-Geräten“ (Nov. 2003) ausdrücklich hin. [www.bfd.bund.de/technik/usb.pdf]

Die kryptografische Verschlüsselung wechselbarer Speichermedien wird auf Anforderung nur für die jeweilige Instanz des Mediums (oder Teile dessen, z.B. einzelne Dateien) angewandt.

Aufgabe

Aufgabe der Erfindung ist es, ein Verfahren zu schaffen, welches unter Beibehaltung der Schnittstellenfunktionalität den unerwünschten Datentransfer mittels wechselbarer Speichermedien verhindert ohne den erwünschten Datentransfer mittels wechselbarer Speichermedien einzuschränken.

Lösung der Aufgabe

Ein in ein Betriebssystem eingebundenes Programm (i.d.R. bestehend aus mehreren Treibern, Filtern, Diensten, etc.) analysiert Protokoll und Datenstrom von und zu Datenträgern, Speichermedien und Peripheriegeräten. Unter Einbeziehung der a priori bekannten, ausgewiesenen oder administrativ deklarierten Eigenschaften und Präferenzen erfolgt eine selbst-

ständige Klassifikation hinsichtlich der Möglichkeit, als wechselbares Speichermedium zu dienen.

Alle als wechselbares Speichermedium tauglichen Datenträger oder Geräte werden mit einer Verschlüsselung belegt. Je nach Implementation werden entweder der Datenträger als Ganzes oder lediglich Dateiinhalte verschlüsselt.

Bei Vorliegen besonderer Identifikationsmerkmale kann die Verschlüsselung temporär außer Kraft gesetzt werden.

Die Verschlüsselung (und Entschlüsselung) erfolgt auf einer sehr niedrigen Ebene, quasi „unmittelbar vor dem Datenträger", so dass sie weder für Anwendungsprogramme noch für das Betriebssystem in Erscheinung tritt.

Vorteile

Die Erfindung ermöglicht die Benutzung wechselbarer Speichermedien ohne dass befürchtet werden muss, dass diese von Unbefugten kompromittiert werden können. Dies gilt nicht nur für Halbleiterspeicher (wechselbare Festplatten, Memory Sticks, etc.) sondern auch für alle „traditionellen" magnetischen, magnetooptischen oder optischen Datenträger (Disketten, Zip, Jaz, Bänder, CD, MO, WORM, etc.).

Es ist nicht erforderlich, Schnittstellen oder Laufwerke abzuschalten oder gar auszubauen. Damit kann die volle Funktionalität der Computerhardware genutzt werden.

Die nicht vorhandene Kopplung von Benutzerauthentifizierung und Schlüsselmanagement macht die Sicherheit der Speichermedien unabhängig von der Sicherheit des Betriebssystems, d. h. unsichere, ausgespähte oder notierte Passworte vermindern die Sicherheit nicht.

Es ist keine Aktion seitens der Benutzer erforderlich, welche durch Fahrlässigkeit oder böse Absicht unterbleiben könnte.

Es ist keine Änderung in der Logik des Betriebssystems oder ein spezielles Dateisystem (etwa EFS, Encrypting File System) erforderlich. Die spezifischen Vorteile der jeweiligen Dateisysteme (z.B. Datenkompression, Zugriffskontrolle*, etc.) bleiben in vollem Umfang erhalten. Der Schutz ist nicht an ein bestimmtes Dateisystem gebunden, sondern ergänzt jedes Dateisystem. (*Die Zugriffskontrolle ist i. A. nur im Binnenverhältnis wirksam, d. h. außenstehende Dritte mit Administrationsberechtigung können die Zugriffskontrolle übernehmen.)

Bei Verlust oder Entwendung von Datenträgern bedeutet dies nicht zugleich den Verlust der Vertraulichkeit der darauf enthaltenen Daten.

Das zur Anwendung kommende kryptografische Verfahren bleibt einem potentiellen Angreifer unbekannt, womit ein Angriff erschwert wird.

Damit wird aus einem potentiell unsicheren Speichermedium ein Speichermedium für besondere Sicherheitsanforderungen, denn besonders sensible Daten können ausschließlich auf wechselbaren Speichermedien gehalten werden, um durch physischen Verschluss vor unbefugtem Zugriff geschützt zu werden

Durch Anwendung dieses Verfahrens auf mehreren Computern mit einem gemeinsamen Schlüssel entsteht eine Sicherheitsdomäne. Dabei ist es nicht erforderlich, dass die Computer einer Sicherheitsdomäne miteinander verbunden sind (z.B. im LAN). Innerhalb einer Sicherheitsdomäne wird die Verschlüsselung wechselseitig aufgehoben, so dass wechselbare Speichermedien (etwa zur Datensicherung) uneingeschränkt verwendet werden können. Die vom Betriebssystem zur Verfügung gestellten Mittel der Zugriffskontrolle bleiben dabei erhalten.

Ansprüche

1. Verfahren zur Verhinderung des Verlustes der Vertraulichkeit von Daten mittels wechselbarer/austauschbarer Speichermedien zur Anwendung in einem beliebigen Betriebssystem **dadurch gekennzeichnet, dass** jedes Dateisystem auf einem wechselbaren Speichermedium um eine kryptografische Verschlüsselung ergänzt und diese - automatisch oder auf Anforderung - auf alle Instanzen dieser Klasse von Speichermedien angewandt wird ohne dass sie für Anwendungsprogramme oder für das Betriebssystem in Erscheinung tritt.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** jedes Dateisystem auf einem nicht wechselbaren/austauschbaren Speichermedium um eine kryptografische Verschlüsselung ergänzt wird.

3. Verfahren nach Anspruch 1 oder Anspruch 2, **dadurch gekennzeichnet, dass** die kryptografische Verschlüsselung bei Vorliegen besonderer Merkmale temporär außer Kraft gesetzt wird.

4. Verfahren zur Bildung eines logischen Zusammenschlusses von Computern zu einer Gruppe, **dadurch gekennzeichnet, dass** durch Anwendung eines Verfahrens der vorherigen Ansprüche innerhalb der Gruppe die kryptografische Verschlüsselung wechselseitig aufgehoben, nach außen hin jedoch aufrecht erhalten wird.

Ausführungsbeispiel

Eine Implementation - beispielsweise für das Betriebssystem Windows - kann dergestalt erfolgen, dass eine Kombination aus geeigneten Filtern und Treibern erstellt wird, die auf sehr niedriger Ebene den Protokoll- und Datenfluss zwischen den Anwendungsprogrammen und höheren Ebenen des Betriebssystems einerseits und den Speichermedien andererseits analysiert und - nach Bedarf - modifiziert. Die Modifikation besteht in der Anwendung einer kryptografischen Verschlüsslung. Sie kann (je nach installierter Option) entweder das Speichermedium als Ganzes, oder Teile davon (Dateiinhalte) verschlüsseln. Die Auswahl der zu überwachenden Schnittstellen und Laufwerke kann produktspezifisch festgelegt oder administrabel sein.

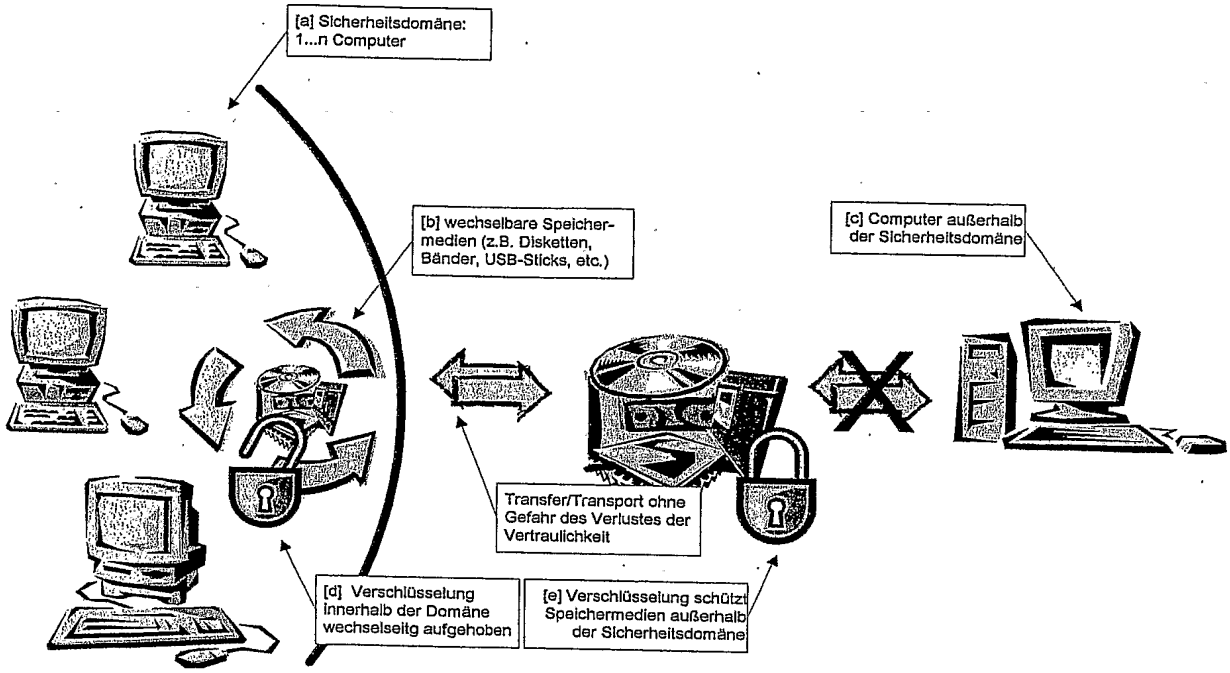
Ein weiterer Dienst fungiert als Schlüsselverwalter für die kryptografische Komponente. Er kann für einzelne Computer die notwendigen Schlüssel in einer geeigneten Datei oder Datenbank verwalten. Für mehrere Computer mit gemeinsamer Schlüsselverwaltung stellt dieser Dienst die Schlüssel entweder ebenfalls aus lokaler Verwaltung zur Verfügung, oder - bei Verbindung beispielsweise im LAN - in Abstimmung mit einem zentralen Schlüsselverwalter.

Bei Vorliegen besonderer Merkmale kann die Verschlüsselung temporär außer Kraft gesetzt werden. Diese Merkmale können durch eine besondere Identifikation - beispielsweise eines physischen Schlüssels - vorliegen; sie können aber auch in den Daten begründet sein. So kann ein sog. Dongle, der nur zeitweise ausgegeben wird, die Verschlüsselung aufheben, um die Erstellung von Datenträgern zur Veröffentlichung zu ermöglichen. Ebenso kann die Erkennung bestimmter Dateiformate die Verschlüsselung aufheben, so dass Bilddaten von einer Kamera gelesen werden können.

Durch Zusammenschluss mehrerer Computer mit gemeinsamer Schlüsselverwaltung entsteht eine Sicherheitsdomäne [a (s. Skizze)]. Dabei ist es nicht notwendig, dass alle Computer miteinander vernetzt sind. So können eine oder mehrere Abteilungen eines Betriebes eine Sicherheitsdomäne bilden. Ebenso können dies mehrere Computer eines Benutzers an unterschiedlichen Standorten sein, zwischen denen Daten per Wechseldatenträger übertragen werden. Wechselbare Speichermedien [b], die innerhalb der Domäne erstellt werden, bzw. einzelne Dateien darauf, die innerhalb der Domäne geschrieben werden, sind mit Computern außerhalb [c] nicht lesbar und umgekehrt [e]. Innerhalb der Domäne können wechselbare Speichermedien freizügig benutzt werden [d].

Beispielszenarien:

- Bandkassetten oder andere zur Datensicherung eingesetzte Speichermedien können dezentral aufbewahrt werden. Besondere Transportsicherungsmaßnahmen entfallen.
- Besonders sensible Daten können ausschließlich auf Wechselfestplatten gehalten werden. Sie können physisch weggeschlossen werden und sind nur innerhalb der Sicherheitsdomäne lesbar.
- Gesetzliche Auflagen hinsichtlich des Datenschutzes lassen sich leichter einhalten, da alle Speichermedien, die die Sicherheitsdomäne verlassen vor unbefugtem Lesen geschützt sind.
- Persönliche oder wirtschaftliche Nachteile können aus dem gleichen Grund vermieden werden.
- In einem LAN können lokale Datensicherungen (auf Clientcomputern) durchgeführt werden. Eine missbräuchliche Nutzung ist nicht zu befürchten.
- Die unkontrollierte Ausführung nicht freigegebener Programme kann unterbunden werden, da der Eintrag via Speichermedien nicht möglich ist (sofern nicht CD-ROMs freigegeben sind).



Skizze zum Ausführungsbeispiel